Hillstone CloudHive asegura una nube privada para un gigantesco Gobierno Provincial

El Cliente

Un gigantesco gobierno provincial que administra una nube privada con más de 30 servidores y más de 300 máquinas virtuales que ejecutan VMWare ESXi 5.5 y 6.0.

La plataforma en la nube ofrece principalmente alojamiento web y servicios de gobierno electrónico para sus más de 50 departamentos gubernamentales subsidiarios ubicados en diferentes lugares.

El Reto

La topología de la red VM del cliente se aprecia en la Figura 1. No hay segmentación o aislamiento entre los diferentes inquilinos; las agencias de previsión meteorológica, las oficinas de estadística, los departamentos de policía y las organizaciones de inversión, etc. comparten las mismas propiedades de red. Lo que es aún más arriesgado es tener servidores web, servidores de aplicaciones y servidores de bases de datos en una red L2 no segmentada. Esto significa que una vez que se vulnera una máquina virtual en un departamento no clasificado, la amenaza podría pasar a otras máquinas virtuales clasificadas o críticas sin ningún punto de control; y una vez que un atacante gana el control de un servidor web, el intruso puede entrar fácilmente a los

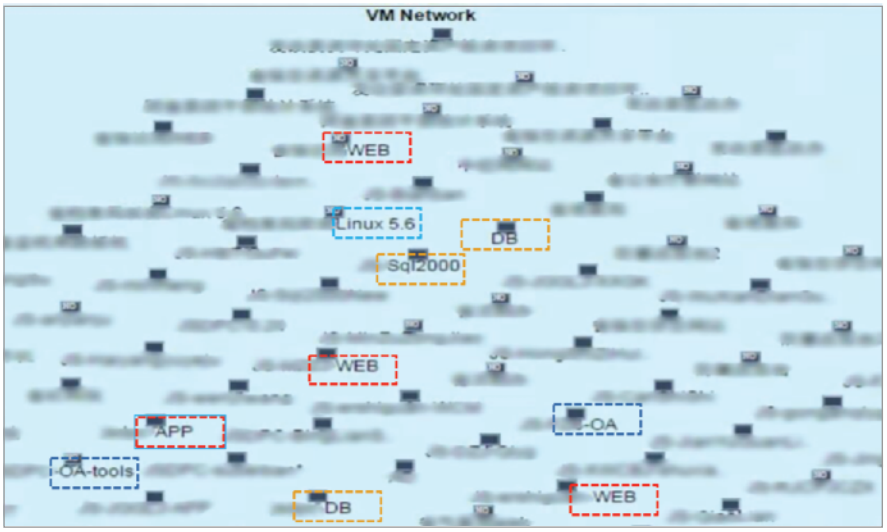

Figura 1: Topología de la Red VM del Cliente

servidores de base de datos para extraer datos, así como registros confidenciales. De hecho, esto ha sucedido en el pasado, y este cliente no fue el único. Cuando un sitio web alojado en su plataforma en la nube estaba comprometido con una inyección de SQL, no tuvieron manera de proteger los servidores de aplicaciones y las bases de datos. El departamento de Informática enfrentó fuerte presión y el equipo comenzó a buscar una solución efectiva que fuera fácil de implementar.

La Solución

Crear VLANs para segmentar diferentes usuarios y máquinas virtuales a través del vCenter podría ser una solución para su situación. Sin embargo, las configuraciones de las VLAN son típicamente muy complejas. Los administradores necesitarían cambiar todas las configuraciones de cada firewall, SW y enrutadores, conectándose individualmente con cada uno de los dispositivos, ya que no se puede configurar centralmente a través del vCenter. Por lo tanto, la VLAN no era una solución viable.

Cuando el equipo de operaciones comenzó a probar la solución de Hillstone CloudHive, encontraron que se puede implementar fácilmente a través del vCenter sin ninguna interrupción de su red, y sin necesidad de configuración adicional alguna en los conmutadores o en los firewalls o incluso en las mismas máquinas virtuales. Los administradores pudieron agregar o quitar servicios CloudHive fácilmente en cada base VM.

Además, CloudHive detectó más de 80.000 eventos de amenaza en la red virtual, que no se habían detectado previamente. Al investigar más a fondo cada amenaza crítica alertada, el administrador encontró fácilmente que la conexión entre un servidor web y el servidor app2 era anormal (resaltado por un enlace rojo en la Figura 2). En efecto, el servidor web estaba ejecutando un enlace de exploración al servidor app2. Con CloudHive, el administrador pudo tomar medidas rápidas para resolver lo del servidor web comprometido.

Además, el administrador encontró que podían añadir seguridad a la red de VMs o VLAN basándose en las prioridades del negocio y configurar políticas de seguridad avanzadas para proteger activos altamente clasificados.

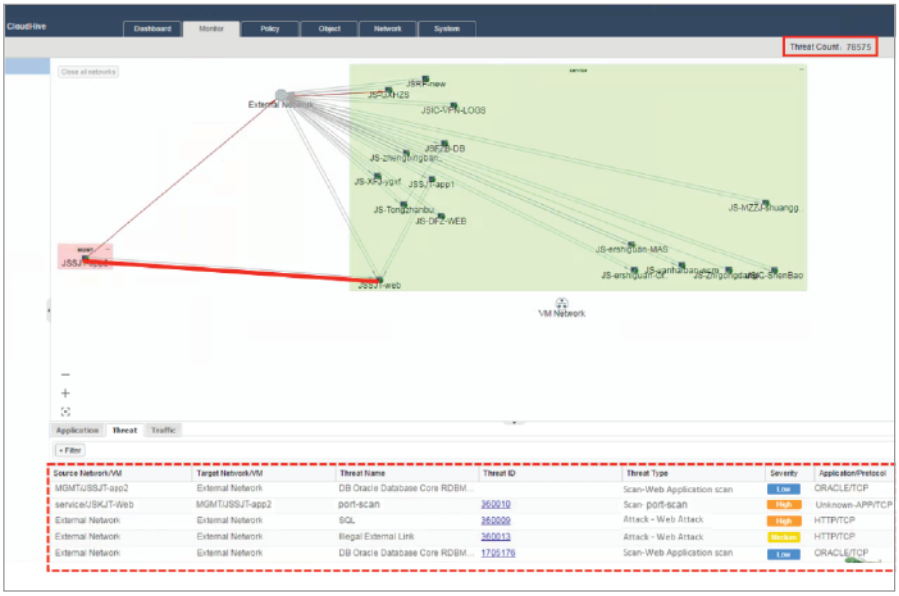

Figura 2: Topología de red VM por capas, después de implementar CloudHive

La Conclusión

Con la solución de micro-segmentación CloudHive, el equipo de operaciones en la nube pudo ejecutar la red virtual de manera efectiva y segura. Al obtener una visibilidad profunda de las redes virtuales, el tráfico, las aplicaciones y las amenazas -profundizando en cada máquina virtual- CloudHive ha permitido al equipo de operaciones tomar medidas de seguridad rápidas para detener las brechas dentro de su despliegue en la nube y así asegurar la integridad de sus activos.

Hillstone NETWORKS

Américas: **+1-800-889-9860** | APAC: **+86-400-828-6655** | Europa: **+420-910-117-735**

Solicitar una versión de prueba o prueba gratuita:
inquiry@hillstonenet.com